

IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
GREENVILLE DIVISION

Jacob Stuart and Donald Dollar,
individually and on behalf of all others
similarly situated,

Plaintiffs,

v.

Kyocera AVX Components
Corporation,

Defendant.

Case No. 6:23-cv-06087-JDA

OPINION AND ORDER

This matter is before the Court on Defendant's motion to dismiss the Consolidated Amended Complaint ("CAC"). [Doc. 26.] For the reasons discussed below, the Court grants the motion.

BACKGROUND¹

Defendant is an American manufacturer of advanced electronic components with headquarters in Fountain Inn, South Carolina. [Doc. 16 at 7 ¶¶ 22–23.²] Plaintiffs and Putative Class Members (collectively, "Plaintiffs") are current and former employees of Defendant who provided confidential personally identifiable information ("PII"), including their names, addresses, Social Security numbers, dates of birth, employee IDs, phone numbers, trade unions, employment compensation, health insurance information, other

¹ The facts included in the Background section are taken directly from the CAC. [Doc. 16.]

² There appears to be a clerical error in the paragraph numbering in the CAC. [See Doc. 16 at 19–20.] To avoid any confusion, the Court will cite to the CAC using page numbers and paragraph numbers.

IDs, genders, and handwritten signatures, to Defendant as a condition of employment. [*Id.* at 8, 11 ¶¶ 28–29, 43.] Defendant represented to Plaintiffs that their PII would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it. [*Id.* at 8 ¶ 31.]

Over the course of six weeks—between February 16, 2023, and March 30, 2023—Defendant learned that it experienced a network security incident during which an unauthorized third party gained access to Defendant’s network environment (the “Cyber Attack”). [*Id.* at 10 ¶ 41.] Upon learning of the incident, Defendant engaged a specialized third-party forensic incident response firm to secure the network environment and investigate the extent of unauthorized activity. [*Id.* at 10–11 ¶ 42.] The investigation revealed that the unauthorized third party obtained PII of Defendant’s employees through the Cyber Attack (the “Data Breach”). [*Id.*] Beginning on October 30, 2023, Defendant sent Plaintiffs and other Data Breach victims a Notice of Security Incident Letter (the “Notice”) informing them of the Data Breach. [*Id.* at 11 ¶ 43.] Plaintiffs allege that their PII was accessed and stolen in the Data Breach and may have been subsequently sold on the dark web following the Data Breach. [*Id.* at 12–13 ¶¶ 48–49.] The CAC further alleges that Plaintiff Dollar has experienced an increase in spam calls, texts, and/or emails that were caused by the Data Breach. [*Id.* at 38 ¶ 124.]

On November 28, 2023, and December 6, 2023, Plaintiff Dollar and Plaintiff Stuart, respectively, filed putative class action complaints against Defendant in this Court. [Doc. 1]; *Stuart v. Kyocera AVX Components Corp.*, 6:23-cv-6332-BHH. On January 18, 2024, the Court granted Plaintiffs’ joint motion to consolidate the cases and closed the

Stuart action. [Doc. 7.] On February 20, 2024, Plaintiffs filed the CAC. [Doc. 16.] The CAC alleges claims for negligence and negligence per se, invasion of privacy, unjust enrichment, breach of implied contract, and breach of fiduciary duty based on Plaintiffs' alleged injuries resulting from the Data Breach. [*Id.* at 48–62 ¶¶ 157–224.] Plaintiffs seek injunctive relief; actual, statutory, nominal, and consequential damages; attorneys' fees, costs, and litigation expenses; prejudgment and/or post-judgment interest; and such other and further relief that this Court deems just and proper. [*Id.* at 63–67.]

On April 5, 2024, Defendant filed a motion to dismiss the CAC. [Doc. 26.] Plaintiffs filed a response on May 13, 2024 [Doc. 37], and Defendant filed a reply on June 12, 2024 [Doc. 38]. The motion is ripe for review.

APPLICABLE LAW

Rule 12(b)(1) Standard

A challenge to standing “implicates this Court’s subject matter jurisdiction and is governed by Rule 12(b)(1).” *Crumbling v. Miyabi Murrells Inlet, LLC*, 192 F. Supp. 3d 640, 643 (D.S.C. 2016). Article III limits a federal court’s jurisdiction to cases and controversies, and “[o]ne element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 408 (2013) (internal quotation marks omitted). To possess Article III standing, a “plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). In a class action, courts “analyze standing based on the allegations of personal injury made by the named plaintiffs.” *Beck v. McDonald*, 848 F.3d 262, 269 (4th Cir. 2017). Additionally, “[s]tanding

is not dispensed in gross,” and instead, “a plaintiff must demonstrate standing for each claim he seeks to press and for each form of relief that is sought.” *Davis v. Fed. Election Comm’n*, 554 U.S. 724, 734 (2008) (internal quotation marks and citation omitted).

“The party attempting to invoke federal jurisdiction bears the burden of establishing standing.” *Miller v. Brown*, 462 F.3d 312, 316 (4th Cir. 2006). When ruling on a motion to dismiss for lack of standing, a court “must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party.” *Warth v. Seldin*, 422 U.S. 490, 501 (1975). “Nevertheless, the party invoking the jurisdiction of the court must include the necessary factual allegations in the pleading, or else the case must be dismissed for lack of standing.” *Bishop v. Bartlett*, 575 F.3d 419, 424 (4th Cir. 2009). “When a defendant raises standing as the basis for a motion under Rule 12(b)(1) . . . the district court may consider evidence outside the pleadings without converting the proceeding to one for summary judgment.” *White Tail Park, Inc. v. Stroube*, 413 F.3d 451, 459 (4th Cir. 2005) (internal quotation marks omitted). “A federal court is powerless to create its own jurisdiction by embellishing otherwise deficient allegations of standing.” *Whitmore v. Arkansas*, 495 U.S. 149, 155–56 (1990).

Rule 12(b)(6) Standard

Under Rule 12(b)(6) of the Federal Rules of Civil Procedure, a claim should be dismissed if it fails to state a claim upon which relief can be granted. When considering a motion to dismiss, the court should “accept as true all well-pleaded allegations and should view the complaint in a light most favorable to the plaintiff.” *Mylan Lab’ys, Inc. v. Matkari*, 7 F.3d 1130, 1134 (4th Cir. 1993). However, the court “need not accept the legal conclusions drawn from the facts” nor “accept as true unwarranted inferences,

unreasonable conclusions, or arguments.” *E. Shore Mkts., Inc. v. J.D. Assocs. Ltd. P’ship*, 213 F.3d 175, 180 (4th Cir. 2000). Further, for purposes of a Rule 12(b)(6) motion, a court may rely on only the complaint’s allegations and those documents attached as exhibits or incorporated by reference. See *Simons v. Montgomery Cnty. Police Officers*, 762 F.2d 30, 31–32 (4th Cir. 1985). If matters outside the pleadings are presented to and not excluded by the court, the motion is treated as one for summary judgment under Rule 56 of the Federal Rules of Civil Procedure. Fed. R. Civ. P. 12(d).

With respect to well pleaded allegations, the United States Supreme Court explained the interplay between Rule 8(a) and Rule 12(b)(6) in *Bell Atlantic Corp. v. Twombly*:

Federal Rule of Civil Procedure 8(a)(2) requires only “a short and plain statement of the claim showing that the pleader is entitled to relief,” in order to “give the defendant fair notice of what the . . . claim is and the grounds upon which it rests.” While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff’s obligation to provide the “grounds” of his “entitle[ment] to relief” requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do. Factual allegations must be enough to raise a right to relief above the speculative level on the assumption that all the allegations in the complaint are true (even if doubtful in fact).

550 U.S. 544, 555 (2007) (footnote and citations omitted); see also 5 Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 1216, at 235–36 (3d ed. 2004) (“[T]he pleading must contain something more . . . than a bare averment that the pleader wants compensation and is entitled to it or a statement of facts that merely creates a suspicion that the pleader might have a legally cognizable right of action.”).

“A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* The plausibility standard reflects the threshold requirement of Rule 8(a)(2)—the pleader must plead sufficient facts to show he is entitled to relief, not merely facts consistent with the defendant’s liability. *Twombly*, 550 U.S. at 557; *see also Iqbal*, 556 U.S. at 678 (“Where a complaint pleads facts that are merely consistent with a defendant’s liability, it stops short of the line between possibility and plausibility of entitlement to relief.” (internal quotation marks omitted)). Accordingly, the plausibility standard requires a plaintiff to articulate facts that, when accepted as true, demonstrate that the plaintiff has stated a claim that makes it plausible the plaintiff is entitled to relief. *Francis v. Giacomelli*, 588 F.3d 186, 193 (4th Cir. 2009).

DISCUSSION

Defendant argues that the CAC should be dismissed for lack of subject matter jurisdiction because Plaintiffs lack standing in that they have not plausibly alleged injury in fact, and, even if they have standing, the CAC should be dismissed for failure to state a claim upon which relief can be granted. [Doc. 26-1.] The Court first addresses Defendant’s arguments regarding standing. *See Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921 (4th Cir. 2022) (“Because standing is a threshold jurisdictional question, we address it first.” (cleaned up)).

Defendant argues that Plaintiffs lack standing because Plaintiffs’ allegations of potential future harm are insufficient, Plaintiffs have failed to plead facts showing they

suffered concrete injuries related to the Data Breach, and Plaintiffs' conclusory request for injunctive relief is insufficient to establish standing for injunctive relief. [Doc. 26-1 at 16–30.] Based on these arguments, Defendant challenges only the first element of the standing analysis—whether Plaintiffs suffered an injury in fact.

To establish the first element of standing, a plaintiff must show that he suffered an injury in fact that is “concrete and particularized” and “actual or imminent.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (internal quotation marks omitted). “The most obvious concrete injuries are tangible harms, such as physical harms and monetary harms. Intangible harms are trickier, but they too can be concrete.” *O’Leary v. TrustedID, Inc.*, 60 F.4th 240, 242 (4th Cir. 2023) (cleaned up).

In response to Defendant’s motion, Plaintiffs argue that the present and continuing threat of identity theft and fraud is “actual or imminent” so as to support standing; that Plaintiffs’ mitigation costs were reasonable and are compensable as concrete injuries; that the diminished value theory of injury supports standing; that their invasion of privacy injury allegations are sufficient to support Article III standing; that the alleged targeted spam satisfies the Article III inquiry; that their emotional distress injuries support standing; that their benefit of the bargain damages are concrete injuries; and that Plaintiffs have standing to pursue injunctive relief. [Doc. 37 at 10–21.] The Court addresses Plaintiffs’ arguments regarding standing seriatim.

Plaintiffs’ Risk of Future Fraud or Identity Theft

Plaintiffs first argue that they have alleged an injury sufficient for Article III standing because they allege that Plaintiffs have faced—and continue to face—a substantial risk of future fraud or identity theft and that harm is certainly impending. [*Id.* at 10–12.]

Specifically, Plaintiffs argue that because they allege that their PII was the object of a targeted cyberattack and that at least one of them has already experienced misuse of his PII by an increase in spam phone calls, they have sufficiently alleged a substantial risk of future fraud or identity theft. [*Id.*]

A threatened injury constitutes an injury in fact when it “is *certainly* impending” or there is a “substantial risk” of future harm. *Clapper*, 568 U.S. at 409, 414 n.5 (internal quotation marks omitted); see *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (citing *Clapper* for the proposition that a threat of future injury is sufficient to confer standing if it is either “certainly impending” or there is a “substantial risk that the harm will occur.” (internal quotation marks omitted)).³ “Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes.” *Beck*, 848 F.3d at

³ It is apparent to this Court that there are two tests for establishing imminence in a standing inquiry: whether the harm is “certainly impending” or whether there is a “substantial risk that the harm will occur.” See *Driehaus*, 573 U.S. at 158 (internal quotation marks omitted); see also Michael B. Jones, *Uncertain Standing: Normative Applications of Standing Doctrine Produce Unpredictable Jurisdictional Bars to Common Law Data Breach Claims*, 95 N.C. L. Rev. 201, 202–03 (2016) (noting that although “*Clapper* approved the ‘certainly impending’ standard as the appropriate measure of a future injury’s cognizability, . . . the Court observed in a footnote that an alternative standard, one that insists on a ‘substantial risk’ of future harm, remains viable”). The Fourth Circuit did not specifically address these alternative standards when analyzing the plaintiffs’ risk of future fraud or identity theft in *Beck*, an opinion upon which this Order largely relies, but the Supreme Court and Fourth Circuit have both applied these dual standards following the Fourth Circuit’s ruling in *Beck*. See, e.g., *Dep’t of Com. v. New York*, 588 U.S. 752, 767 (2019) (holding that future injuries “may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur” (internal quotation marks omitted)); *John & Jane Parents 1 v. Montgomery Cnty. Bd. of Educ.*, 78 F.4th 622, 629 (4th Cir. 2024) (holding that the injury in fact “prong requires either a current injury, a certainly impending injury, or a substantial risk of a future injury”). Accordingly, the Court will analyze Plaintiffs’ allegations of risk of future harm under both the “certainly impending” standard and the “substantial risk of future injury” standard.

271 (internal quotation marks omitted). Sufficiently imminent injuries in fact cannot be premised on a “highly attenuated chain of possibilities.” *Clapper*, 568 U.S. at 410.

Fourth Circuit Precedent

The Fourth Circuit has clarified that “being subjected to a data breach isn’t in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft.” *O’Leary*, 60 F.4th at 244. Although the Fourth Circuit has not issued an opinion regarding standing in a case with facts identical to those presented here, two recent Fourth Circuit decisions are instructive. The Fourth Circuit first addressed the issue of whether an increased risk of fraud or identity theft constitutes an Article III injury in fact in *Beck*, 848 F.3d at 273–76. *Beck* was a consolidated appeal of two cases regarding data breaches at a veterans’ affairs medical center: the first involved a stolen laptop containing the plaintiffs’ personal identifying information and the second involved a box of missing documents containing the plaintiffs’ personal identifying information. 848 F.3d at 266, 268. The plaintiffs in both cases argued that the increased risk of identity theft following these incidents constituted an injury in fact. *Id.* at 266–67. The Fourth Circuit disagreed. *Id.* at 267, 275. Acknowledging a circuit split regarding whether standing can be premised merely on an “increased risk of future identity theft,” the Fourth Circuit concluded that the plaintiffs failed to meet *Clapper*’s requirement that threatened injury be “certainly impending” because they did not allege any actual misuse of their personal identifying information. *Id.* at 273–75. Moreover, the potential harm of identity theft as alleged by the plaintiffs would have required the Fourth Circuit to speculate regarding an “attenuated chain of possibilities” by presuming that the data thief targeted the stolen items because they contained personal identifying information, that the thief

would select the named plaintiffs' personal identifying information, and that the thief would successfully use that information to steal their identities. *Id.* at 275.

In addressing the circuit split on the issue, the Fourth Circuit reviewed cases where courts found that the increased risk of identity theft satisfied the injury-in-fact requirement, noting that the plaintiffs in those cases made allegations sufficient to "push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Id.* at 274. Specifically, in some of those cases, the courts explained that the plaintiffs alleged that the data thief intentionally targeted the plaintiffs' personal identifying information, *id.* (citing *Galaria v. Nationwide Mut. Ins.*, 663 F. App'x 384, 386 (6th Cir. 2016); *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 694 (7th Cir. 2015),; *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 632 (7th Cir. 2007)), and in others, at least one named plaintiff alleged actual misuse or access of the personal identifying information, *id.* (citing *Remijas*, 794 F.3d at 690; *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141 (9th Cir. 2010)). In contrast, the Fourth Circuit concluded that the *Beck* plaintiffs' risk of future identity theft was "too speculative" under *Clapper* and affirmed the district court's dismissal of the cases for lack of standing. *Id.*

A similar issue arose before the Fourth Circuit the next year in *Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018). Unlike the plaintiffs in *Beck*, however, the *Hutton* plaintiffs *did* allege misuse of their stolen personal identity information by alleging that their personal information had been used "to open Chase Amazon Visa credit card accounts without their knowledge or approval." 892 F.3d at 622. Relying on *Beck*, the district court dismissed the case for lack of standing, but the Fourth Circuit disagreed. *Id.* at 616. The Fourth Circuit re-emphasized "that a mere compromise

of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft,” but distinguished *Beck*, explaining:

In *Beck*, the plaintiffs alleged only a threat of future injury in the data breach context where a laptop and boxes—containing personal information concerning patients, including partial social security numbers, names, dates of birth, and physical descriptions—had been stolen, but the information contained therein had not been misused. The Plaintiffs in these cases, on the other hand, allege that they have already suffered actual harm in the form of identity theft and credit card fraud.

Id. at 621–22. Thus, the Fourth Circuit concluded that the plaintiffs’ allegations of actual misuse of their stolen personal information satisfied Article III’s standing requirements by alleging an actual, concrete injury. *Id.* at 622.

Analysis

Here, Plaintiffs do not allege facts to support any actual misuse of their PII, such as a sale of their PII to third parties, identity theft, or unauthorized charges on their credit cards.⁴ Actual misuse of Plaintiffs’ PII, however, may not be strictly required to establish standing in the data breach context. As the Fourth Circuit noted in *Beck*, other circuits have held that a plaintiff may establish standing where he alleges that his personal information was the specific target of the attack.⁵ 848 F.3d at 274 (citing cases).

⁴ Plaintiffs’ conclusory allegation regarding Dollar’s receipt of increased spam phone calls and/or emails is insufficient to support a finding of risk of future harm for the same reasons that it is insufficient to independently confer standing, as discussed below. See discussion *infra* at 17–18 & n.9

⁵ The Fourth Circuit has not yet addressed the specific issue of whether allegations that a plaintiff’s PII was specifically targeted by an unauthorized party—absent allegations of actual misuse—is enough to confer standing. A survey of recent circuit court opinions reveals that allegations of specific targeting are generally at least *considered* in determining whether fraud or identity theft are “certainly impending” or there is a

However, even assuming such an argument would succeed in the Fourth Circuit, Plaintiffs' allegations nonetheless fall short.

Although the CAC states in a conclusory fashion that Plaintiffs "had their most sensitive personal information accessed, exfiltrated, and stolen" [Doc. 16 at 1–2 ¶ 2], there are no factual allegations sufficient to establish that their PII was actually targeted in this way. To be sure, the CAC alleges that "[t]he attacker accessed and acquired files Defendant shared with a third party containing unencrypted [PII] of Plaintiffs" and that an "investigation determined that the unauthorized party obtained [PII] as a result." [*Id.* ¶¶ 42, 48.] But none of these allegations lead to the conclusion that the unauthorized

substantial risk thereof. *See, e.g., McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 301–03 (2d Cir. 2021) (surveying cases). However, most circuit court cases that have considered allegations of specific targeting also involved some allegations of actual misuse, whether affecting a named plaintiff or other victims, and the courts therefore did not analyze in their opinions what allegations of targeting, if any, would be sufficient to confer standing on their own. *See, e.g., Remijas*, 794 F.3d at 692–94 (plaintiffs alleged that personal data had "already been stolen" and that "9,200 cards [] experienced fraudulent charges"); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027–28 (9th Cir. 2018) (concluding that where other plaintiffs suffered financial losses and other harm as a result of the data breach at issue, "their alleged harm undermines [the defendant's] assertion that the data stolen in the breach cannot be used for fraud or identity theft" against the plaintiffs); *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 58 (D.C. Cir. 2019) ("[A] hacker's intent to use breach victims' personal data for identity theft becomes markedly less important where, as here, several victims allege that they have *already* suffered identity theft and fraud as a result of the breaches . . . [including] fraudulent accounts opened and tax returns filed in their names."). One exception is *Galaria v. Nationwide Mutual Insurance*, 663 F. App'x 384, 388 (6th Cir. 2016), cited by *Beck*, in which the Sixth Circuit held in an unpublished opinion that the plaintiffs had alleged a substantial risk of future harm because "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in [the plaintiffs'] complaints." However, relevant to its holding, the court in *Galaria* also concluded that the company's offer to provide credit monitoring services was evidence that there was a substantial risk of future harm, *see id.* at 388–89, which this Court disagrees with under Fourth Circuit precedent, *see discussion infra* at 14, 15.

third party was specifically targeting Plaintiffs' PII, as opposed to other sensitive data. *Cf. Beck*, 848 F.3d at 269 (holding that allegations of theft of data or files containing personal identifying information is not enough to confer standing). Indeed, when describing the Data Breach, Plaintiffs merely allege that their PII was "includ[ed]" in the stolen data and was obtained "as a result" of the Data Breach. [*Id.* ¶¶ 42, 48.]

Further, Plaintiffs' theory of standing would still require several analytical jumps to show that fraud or identity theft was "certainly impending," including that the unauthorized third party actually sold Plaintiffs' PII on the "dark web,"⁶ that it was purchased by a bad actor, and that the bad actor has been waiting, for nearly two years, to steal Plaintiffs' identities or otherwise misuse the PII. This "attenuated chain" demonstrates that the CAC does not plausibly allege that harm is certainly impending. *Beck*, 848 F.3d at 275.

Nor does the CAC plausibly allege a substantial risk that harm will occur. At the outset, this Court follows *Beck* in declining to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals, see 848 F.3d at 276, despite Plaintiffs' allegation that Defendant's offering of credit monitoring and identity theft restoration services is an acknowledgement of imminent threat of future fraud or identity theft [Doc. 16 at 13 ¶ 52]. Further, as discussed above, Plaintiffs have not alleged that any of the data breach victims have already experienced the misuse of their data, nor have they alleged facts showing that their PII was specifically targeted in the attack.

⁶ The CAC includes a conclusory allegation that Plaintiffs' PII was "subsequently sold on the dark web" but does not allege facts to support that contention other than that it "is the modus operandi of cybercriminals." [Doc. 16 at 13 ¶ 49.]

Because Plaintiffs have not sufficiently alleged either that there is a substantial risk of fraud or identity theft or that such harm is certainly impending, the Court concludes that Plaintiffs do not have standing based on their risk of future fraud or identity theft.⁷

Plaintiffs' Mitigation Costs

Plaintiffs also argue that their mitigation efforts constitute injury in fact because their expenses were in response to a “very real threat” that their PII would be misused to commit identity theft and fraud. [Doc. 37 at 14–15.]

The Supreme Court has held that standing cannot be based on precautionary expenses when harm was not certainly impending and there was no substantial risk that harm would occur. *See Clapper*, 568 U.S. at 415 n.5, 416. “In other words, [the plaintiffs] cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm.” *Id.* Similarly, in the data breach context, the Fourth Circuit held in *Beck* that “self-imposed harms,” such as “the cost of measures to guard against identity theft, including the costs of [purchasing] credit monitoring services” “cannot confer

⁷ Because Plaintiffs have not demonstrated an injury in fact based on their risk of future fraud or identity, Plaintiffs also lack standing to pursue injunctive relief. *See Transunion LLC*, 594 U.S. at 435 (“[A] plaintiff must demonstrate standing separately for each form of relief sought.” (internal quotation marks omitted)). Plaintiffs’ conclusory allegation that Defendant does not have “adequate safeguards” to protect Plaintiffs’ PII [Doc. 16 at 52 ¶ 177], without more, is insufficient to establish standing for injunctive relief. *See Beck*, 848 F.3d at 277 (“[T]hese past events, disconcerting as they may be, are not sufficient to confer standing to seek injunctive relief” because “[t]he most that can be reasonably inferred . . . is that the [p]laintiffs *could* be victimized by a future data breach” and “[t]hat alone is not enough.”); *see also Holmes v. Elephant Ins.*, No. 3:22cv487, 2023 WL 4183380, at *6 (E.D. Va. June 26, 2023) (holding that plaintiffs in a data breach case lacked standing to seek declaratory and injunctive relief because they “made only conclusory statements and [did] not articulate[] a sufficiently imminent and substantial risk of another [] data breach.”), *appeal filed*, No. 23-1782, 2023 WL 4183380 (4th Cir. July 28, 2023).

standing” when the “certainly impending” and “substantial risk” standards are not met. 848 F.3d at 276–77.

Here, Plaintiffs have alleged nothing more than self-imposed precautionary expenses that are insufficient, by themselves, to confer standing. Moreover, Plaintiffs allege that they were offered complimentary credit monitoring and identity theft protection services for 12 months by Defendant but do not allege that they enrolled in these services, further discrediting their need for damages for future self-imposed costs of such services. [Compare Doc. 16 at 48 ¶ 156 with Doc. 16 at 5 ¶ 11.]

Diminution in Value of Plaintiffs’ PII

Next, Plaintiffs argue that they suffered a concrete economic injury because the value of their PII diminished as a result of the Data Breach. [Doc. 37 at 15–16.] Plaintiffs contend that this alleged diminution in value constitutes a concrete injury because they have demonstrated the existence of a marketplace in which they could sell their PII. [*Id.* at 16.]

“The Fourth Circuit has not explicitly decided whether the loss of property value in PII constitutes a cognizable injury in data breach cases.” *Darnell v. Wyndham Cap. Mortg., Inc.*, No. 3:20-CV-00690-FDW-DSC, 2021 WL 1124792, at *5 (W.D.N.C. Mar. 24, 2021) (cleaned up). As the Eastern District of Virginia has recognized, “courts that are willing to consider diminution in the value of PII as a basis for standing do so when there are allegations of some concrete injury, such as lower credit scores or fraudulent accounts and tax returns filed in [the] plaintiff’s name.” *Podroykin v. Am. Armed Forces Mut. Aid Assoc.*, 634 F. Supp. 3d 265, 272 (E.D. Va. 2022) (cleaned up).

Here, although the CAC sufficiently alleges that Plaintiffs' PII had financial value and that a marketplace exists for such information [Doc. 16 at 28–29 ¶¶ 88–92], it fails to allege any facts explaining how Plaintiffs actually lost value because of the disclosure of their PII, *see Podroykin*, 634 F. Supp. 3d at 272 (concluding that the plaintiff could not argue that the value of his PII had been diminished because he could not “even allege that his PII had been misused”); *see also Blood v. Labette Cnty. Med. Ctr.*, No. 5:22-cv-04036-HLT-KGG, 2022 WL 11745549, at *6 (D. Kan. Oct. 20, 2022) (“Even if Plaintiffs' PII [] ha[s] monetary value, as Plaintiffs allege, they do not allege facts explaining how they lost value because of the breach. They do not allege (nor likely would they) that they tried to sell their information and couldn't or were offered less than its value.”); *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016) (“This Court need not decide whether such personal information has a monetary value, as Plaintiffs have not alleged that they have attempted to sell their personal information or that, if they have, the data breach forced them to accept a decreased price for that information.”). Accordingly, Plaintiffs have not pled standing based on the diminution in value of their PII.

Invasion of Plaintiffs' Privacy

Plaintiffs next argue that their allegations of invasion of privacy are independently sufficient to support Article III standing. [Doc. 37 at 17.]

Invasion of privacy claims in South Carolina may be broken down into three separate causes of action: wrongful appropriation of personality, wrongful publicizing of private affairs, and wrongful intrusion into private affairs. *Doe 2 v. Associated Press*, 331 F.3d 417, 421 (4th Cir. 2003). Plaintiffs do not specify which cause of action their invasion of privacy claim is based on, but from the allegations in the CAC, the Court construes the

Complaint as asserting the wrongful intrusion into private affairs. [Doc. 16 at 54–56 ¶¶ 186–97.]

The Court of Appeals of South Carolina has noted that “[i]n an action for wrongful intrusion into private affairs, the damage consists of the unwanted exposure resulting from the intrusion.” *Snakenberg v. Hartford Cas. Ins.*, 383 S.E.2d 2, 6 (S.C. Ct. App. 1989). And the Supreme Court of South Carolina has held that where “a plaintiff bases an action for invasion of privacy on intrusion, bringing forth no evidence of public disclosure, it is incumbent upon him to show a blatant and shocking disregard of his rights, and serious mental or physical injury or humiliation to himself resulting therefrom.” *O’Shea v. Lesser*, 416 S.E.2d 629, 633 (S.C. 1992) (internal quotation marks omitted). Here, Plaintiffs have not alleged that they have suffered any serious mental or physical injury or humiliation resulting from the alleged intrusion.⁸ [See Doc. 16 at 54–56 ¶¶ 186–97.] Accordingly, they have not pled standing based on the wrongful intrusion into private affairs.

Plaintiffs’ Injuries Related to Targeted Spam

Plaintiffs also argue that their allegations that Dollar began to receive spam messages via calls, texts, and/or emails as a result of the Data Breach support standing. [Doc. 37 at 18; see Doc. 16 at 38 ¶ 124.] However, Plaintiffs provide no factual support—including the dates or substance of the alleged calls or emails—to sufficiently allege an injury in fact. See *Burger v. Healthcare Mgmt. Sols., LLC*, No. RDB-23-1215, 2024 WL 473735, at *6 (D. Md. 2024) (“[G]eneric allegation[s] of increased spam calls and emails,

⁸ Additionally, the Fourth Circuit has recognized that it is “the unwanted intrusion into the home that marks intrusion upon seclusion,” which is why it has held that unwanted phone calls in violation of the Telephone Consumer Protection Act are concrete injuries in fact. *O’Leary*, 60 F.4th at 245–46.

if [] injur[ies] at all, fail[] to plausibly show that [the plaintiffs'] alleged injuries were the result of [the] [d]efendant's conduct." (internal quotation marks omitted)).⁹ Accordingly, the Court declines to conclude that Plaintiffs' bare allegation regarding an increase in spam calls and/or emails is sufficient to establish Article III standing.

Plaintiffs' Emotional Distress Injuries

Plaintiffs further argue that their alleged emotional distress injuries support standing. [Doc. 37 at 18–19.]

The Fourth Circuit has squarely rejected claims of "emotional upset" and "fear of identity theft and financial fraud" resulting from a data breach as insufficient to confer Article III standing. *Beck*, 848 F.3d at 272 (cleaned up); see also *Stamat v. Grandizio Wilkins Little & Matthews, LLP*, No. SAG-22-00747, 2022 WL 3919685, at *7 (D. Md. Aug. 31, 2022) (declining to confer standing where the plaintiff merely alleged "emotional

⁹ Plaintiffs cite to several cases holding that receipt of spam constitutes an injury for the purpose of establishing standing. [Doc. 37 at 18.] However, nearly all the cited cases involve allegations of actual misuse or concrete injury. See *Solomon v. ECL Grp., LLC*, No. 1:22-CV-526, 2023 WL 1359662, at *1, *4 (M.D.N.C. Jan. 31, 2023) (concluding that the plaintiff's injury was sufficient to satisfy Article III standing because she alleged that she had to change her phone numbers and passwords as a result of an increase in spam texts, calls, and emails); *Farley v. Eye Care Leaders Holdings, LLC*, No. 1:22-CV-468, 2023 WL 1353558, at *4 (M.D.N.C. Jan. 31, 2023) (holding that allegations that there was an authorized charge on one plaintiff's credit card and another's credit score unexpectedly plummeted, together with allegations of an increase in spam emails and texts, were sufficient to satisfy Article III standing); *In re GE/CBPS Data Breach Litig.*, No. 20 Civ. 2903 (KPF), 2021 WL 3406374, at *6 (S.D.N.Y. Aug. 4, 2021) (holding that allegations that class members had already suffered identity theft, fraud, and abuse, in addition to the plaintiff receiving phishing and scam emails, were enough to establish standing). Moreover, the Court does not consider the holding in *Baldwin v. National Western Life Insurance*, No. 2:21-CV-04066-WJE, 2021 WL 4206736, at *4 (W.D. Mo. Sept. 15, 2021), because the court in *Baldwin* appeared to rely on the fact that the defendant could not point to any case law to support the proposition that there must be a closer link between the data breach and alleged spam phone calls and emails than what was alleged, which is not the case here. [See Doc. 26-1 at 27 (citing cases).]

distress” and “lost time, annoyance, interference, and inconvenience” without alleging facts to support these emotional injuries (internal quotation marks omitted)); *cf. TransUnion LLC v. Ramirez*, 594 U.S. 413, 436 n.7 (2021) (“We take no position on whether or how . . . an emotional or psychological harm could suffice for Article III purposes.”). Thus, Plaintiffs’ allegations that they have suffered “significant fear, anxiety, and stress,” as well as loss of sleep [Doc. 16 at 35, 38 ¶¶ 114, 125], are insufficient to support standing.

Plaintiffs’ Being Deprived of the Benefit of Their Bargain

Next, Plaintiffs argue that they have standing because they were deprived of the benefit of their bargain. [Doc. 37 at 19–20.] More specifically, Plaintiffs contend that they would not have provided their PII had they known it would not be protected. [*Id.* at 20 (citing Doc. 16 at 6, 35–36 ¶¶ 21, 112, 119).]

“[T]he Fourth Circuit has never held that an overpayment benefit-of-the-bargain theory in a data breach context is sufficient to confer standing.” *Podroykin*, 634 F. Supp. 3d at 272. Moreover, “even courts willing to entertain this theory of standing consistently reject this theory in data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach.” *Id.* (cleaned up). For example, in *Podroykin*, the complaint alleged that “had [the plaintiff] known that [the defendant] was vulnerable to a cyber-attack, he would not have purchased or would have paid less for the insurance policy” he had purchased from the defendant. *Id.* (internal quotation marks omitted). However, the complaint did not allege “that the actual value of the insurance policy ha[d] decreased.” *Id.* The failure to allege that the actual value of the insurance policy had decreased led the court to conclude that

the complaint failed to allege facts sufficient to confer standing based on the benefit-of-the-bargain injury. *Id.*; see also *Chambliss*, 189 F. Supp. 3d at 572 (concluding that the plaintiffs did not have standing based on a benefit-of-the-bargain injury where they “ma[d]e no allegations that the data breach diminished the value of the health insurance they purchased from” the defendant and offered “no factual allegations indicating that the prices they paid for health insurance included a sum to be used for data security, and that both parties understood that the sum would be used for that purpose”).

Here, like the complaints in *Podroykin* and *Chambliss*, which did not allege that the value of the items the plaintiffs purchased from the defendants was diminished, the CAC does not sufficiently allege that the value of Plaintiffs’ employment positions with Defendant was diminished because of the disclosure of Plaintiffs’ PII. Instead, the Complaint includes only the conclusory allegation that Plaintiffs applied for positions with Defendant with the expectation that Defendant would protect their PII and that they “received employment positions of lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.” [Doc. 16 at 34 ¶ 110.] Such allegations are insufficient to support standing based on a benefit-of-the-bargain injury theory.¹⁰ See also *Blood*, 2022 WL 11745549, at *6 (citing cases and rejecting the

¹⁰ The Court recognizes that a recent decision from the Middle District of North Carolina concluded that the plaintiff had sufficiently alleged that she suffered a concrete injury in fact in the form of lost benefit of the bargain. *Williams v. Dukehealth*, No. 1:22-cv-727, 2024 WL 898051, at *4 (M.D.N.C. Mar. 1, 2024). Notably, neither *Williams* nor the District of Maryland case it cites for the proposition that lost benefit of the bargain may be an injury sufficient to confer standing in a data-breach case cite to a Fourth Circuit case relying on this theory of injury to confer standing. See *id.*; *In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 463 (D. Md. 2020) (noting that “[t]he Fourth Circuit has not addressed this issue” of whether plaintiffs adequately allege “injury-in-fact based on failure to receive the benefit of their bargain regarding data

argument that the plaintiffs established standing by alleging that they overpaid for medical services where a portion of their payment for those services was allegedly for data security); *Austin-Spearman v. AARP & AARP Servs., Inc.*, 119 F. Supp. 3d 1, 14 (D.D.C. 2015) (“This Court finds that, having not established that she actually lost any of the value of her membership, [the plaintiff] has not plausibly claimed that she overpaid for the AARP membership agreement such that she was injured economically and now has standing to sue.”).

Conclusion Regarding Standing

Based on the above, the Court concludes that Plaintiffs lack standing to bring their claims in this case. Although some cases have reached a different conclusion regarding standing in data compromise cases, as noted, most of those cases involve allegations of not only the disclosure of PII, but actual misuse of that information. See *Williams*, 2024 WL 898051, at *4; *In re Marriott Int’l*, 440 F. Supp. 3d at 457; see also *Smith v. Loyola Univ. Med. Ctr.*, No. 23 CV 15828, 2024 WL 3338941, at *2, 4 (N.D. Ill. July 9, 2024) (recognizing that the named plaintiffs received targeted medical advertising related to their medical conditions and prescriptions and concluding that the plaintiffs had standing to pursue claims for damages and injunctive relief). Moreover, most of the case law Plaintiffs cite to support their argument that they have pled an injury in fact sufficient for Article III standing is from outside the Fourth Circuit [see Doc. 37 at 10–21], but this Court

security”). Additionally, in both of those cases, the plaintiffs alleged actual misuse of disclosed information. *Williams*, 2024 WL 898051, at *4 (“Plaintiff has alleged not just the disclosure of her personal health information, but its misuse by Facebook in targeted advertising.”); *In re Marriott Int’l*, 440 F. Supp. 3d at 457 (noting that the stolen “information ha[d] already been misused in some cases”).

is bound by Fourth Circuit precedent. As the Fourth Circuit has explained regarding its data-breach precedents,

In *Beck v. McDonald*, we held that plaintiffs whose personal information was compromised in a data breach hadn't shown an Article III injury based on an alleged "increased risk of future identity theft and the cost of measures to protect against it." 848 F.3d 262, 267 (4th Cir. 2017). The plaintiffs' alleged increased risk was only speculative, and even though a laptop and reports with their personal information had been stolen, "the mere theft of these items, without more, cannot confer Article III standing." *Id.* at 275.

In contrast, the plaintiffs in *Hutton v. National Board of Examiners in Optometry, Inc.*, were, in fact, victims of identity theft traceable to the defendant's data breach. 892 F.3d 613, 621–22 (4th Cir. 2018). Unlike the *Beck* plaintiffs, who relied on "a mere compromise of personal information," the *Hutton* plaintiffs suffered identity theft and credit-card fraud such that there was "no need to speculate on whether substantial harm will befall" them—it already had. *Id.* at 621–22. So those plaintiffs had standing.

O'Leary, 60 F.4th at 244. Given the Fourth Circuit's guidance that "the mere theft of [personal information], without more, cannot confer Article III standing," *Beck*, 848 F.3d at 275, and "a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft," *Hutton*, 892 F.3d at 621, the Court concludes that Plaintiffs lack Article III standing because their claims are limited to the alleged disclosure of their PII, see *O'Leary*, 60 F.4th at 244–46; cf. *Bruce v. T-Mobile USA, Inc.*, No. 2:21-cv-895-BHH, 2023 WL 2011460, at *2 (D.S.C. Feb. 14, 2023) ("[B]ecause [the p]laintiff has alleged nothing more than a mere compromise of personal information, without more, the Court agrees with the Magistrate Judge that he lacks Article III standing at this time."), *appeal dismissed*, No. 23-1785, 2023 WL 9421694 (4th Cir. Oct. 30, 2023); *Betz v. St. Joseph's/Candler Health Sys., Inc.*, 630 F. Supp. 3d 734, 751–

52 (D.S.C. 2022) (“[A]lthough [the p]laintiff alleges that her personal information was targeted and stolen for nefarious purposes, . . . [the p]laintiff does not allege any actual misuse of her information, and the Court ultimately finds that [the p]laintiff’s allegations fail to show that a risk of future harm is ‘certainly impending’ or concrete as opposed to merely speculative.”). Therefore, the Court grants Defendant’s motion to dismiss for lack of subject matter jurisdiction pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure.¹¹

CONCLUSION

Wherefore, based upon the foregoing, Defendant’s motion to dismiss [Doc. 26] is GRANTED, and this case is DISMISSED without prejudice.

IT IS SO ORDERED.

s/ Jacquelyn D. Austin
United States District Judge

March 06, 2025
Greenville, South Carolina

¹¹ Because the Court concludes that Plaintiffs lack standing, it declines to address Defendant’s alternative arguments for dismissal based on failure to state a claim. See *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 94 (1998) (recognizing that “[w]ithout jurisdiction the court cannot proceed at all in any cause” and “the only function remaining to the court is that of announcing” the lack of jurisdiction “and dismissing the cause” (internal quotation marks omitted)); *O’Leary*, 60 F.4th at 242 (stating that, because the plaintiff alleged no Article III injury, the court could not—and would not—reach the question of whether he had pled facts to state a claim for relief).